

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-214482

(43)Date of publication of application : 15.08.1997

(51)Int.Cl.

H04L 9/30  
G09C 1/00

(21)Application number : 08-016707

(71)Applicant : NIPPON TELEGR & TELEPH  
CORP <NTT>

(22)Date of filing : 01.02.1996

(72)Inventor : KUWAKADO SHUSUKE  
KOYAMA KENJI

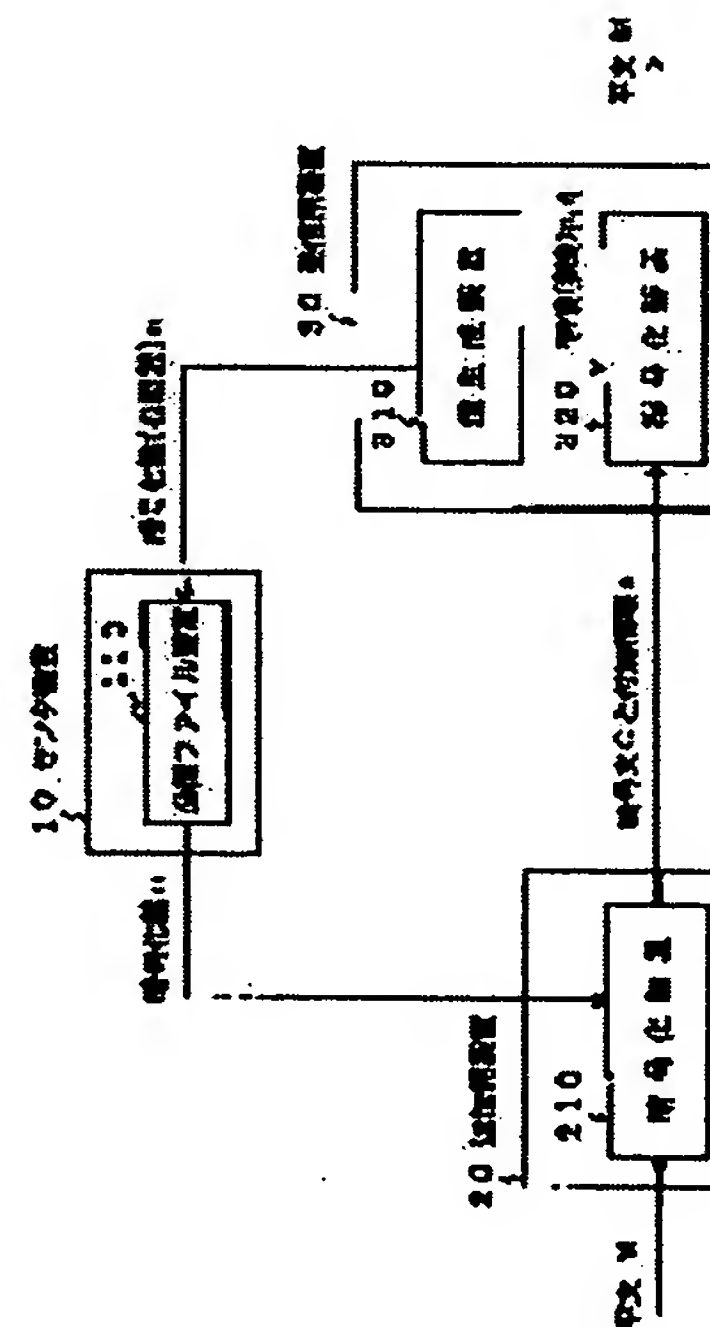
## (54) PUBLIC KEY CIPHERING METHOD AND PUBLIC KEY CIPHERING COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To make difficulty of decoding equivalent to difficulty of factorization into prime factors, to attain definite decoding with additional information of a simple calculation and to attain high speed decoding.

SOLUTION: A key generator 310 generates two primes  $p$ ,  $q$ , to obtain  $n=pq$ , and a value ( $n$ ) is registered in a public file device 110 as a ciphering key and the values  $p$ ,  $q$  are stored in a decoder 320 as decoding keys. A ciphering device 210 uses the ciphering key ( $n$ ) and a plain text  $M$ , a point  $C=(cx, cy)$  obtained doubling the plain text  $N=(mx, my)$  on an ellipse by  $2=x^3+x \pmod n$  is used for a ciphered text and additional information ( $e$ ) and the ciphered text are sent. A decoder 320 uses

decoding keys  $p$ ,  $q$  to apply a multiple of  $1/2$  to the ciphered text  $C$  on the ellipse by  $2=x^3+x \pmod p$ ,  $q$  to obtain objects  $M1(i=1-4)$ . In this case, a formula of a solution of a quartic equation is used. The plain text  $M$  is selected by using the additional information ( $e$ ) from the objects  $M1$ .



## LEGAL STATUS

[Date of request for examination] 01.02.1996

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number] 2836059

[Date of registration] 09.10.1998

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-214482

(43) 公開日 平成9年(1997)8月15日

(51) Int.Cl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/30			H 0 4 L 9/00	6 6 3 A
G 0 9 C 1/00	6 2 0	7259-5 J	G 0 9 C 1/00	6 2 0 A

審査請求 有 請求項の数 2 O L (全 9 頁)

(21) 出願番号 特願平8-16707

(22) 出願日 平成8年(1996)2月1日

特許法第30条第1項適用申請有り 1995年12月14日 社団法人電子情報通信学会開催の「情報セキュリティ研究会」において文書をもって発表

(71) 出願人 000004226

日本電信電話株式会社  
東京都新宿区西新宿三丁目19番2号

(72) 発明者 桑門 秀典

東京都新宿区西新宿三丁目19番2号 日本電信電話株式会社内

(72) 発明者 小山 謙二

東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

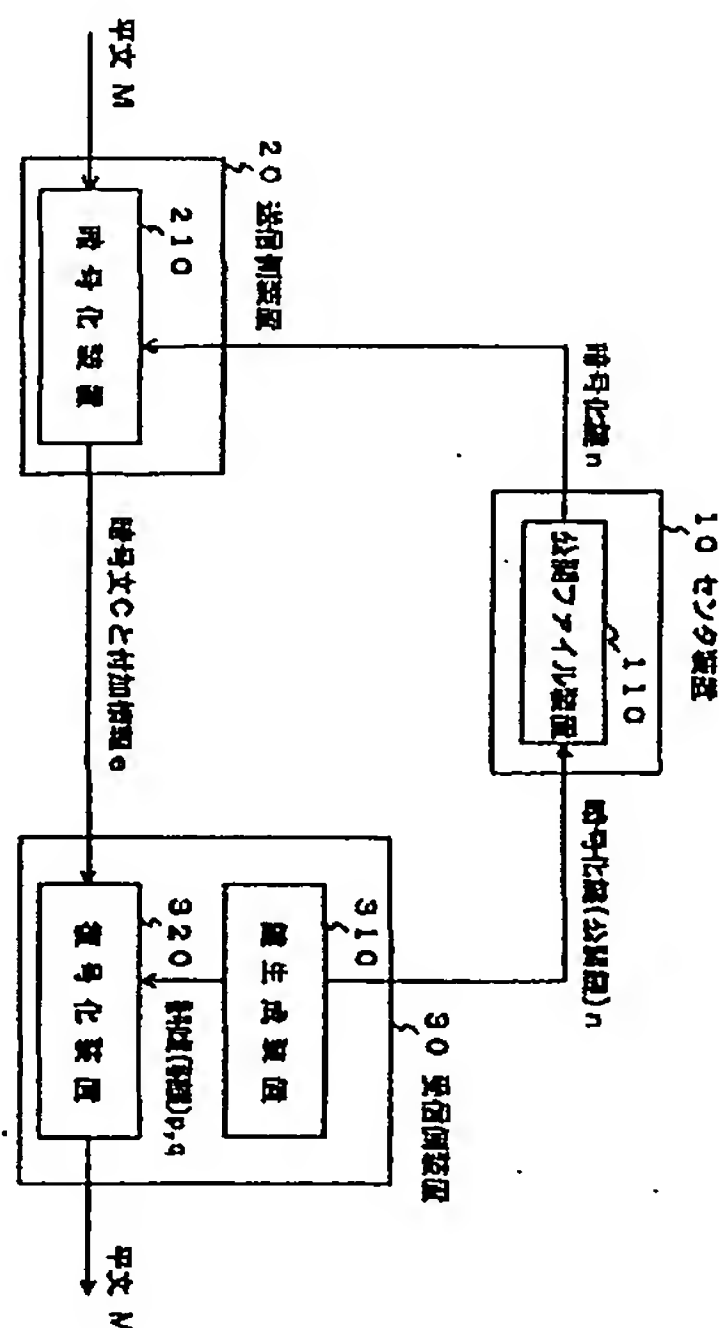
(74) 代理人 弁理士 鈴木 誠

(54) 【発明の名称】 公開鍵暗号方法及び公開鍵暗号通信システム

(57) 【要約】

【課題】 解読の難しさが素因数分解の難しさと等価であり、かつ簡単な計算の付加情報で一意的復号を可能とし、さらに高速な復号化を可能とする。

【解決手段】 鍵生成装置310は、2つの素数 $p$ 、 $q$ を生成し、 $n=pq$ を求め、 $n$ を暗号化鍵として公開ファイル装置110に登録し、 $p$ と $q$ を復号化鍵として復号化装置320で記憶する。暗号化装置210は、暗号化鍵 $n$ と平文 $M$ により、平文 $M=(m_x, m_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{n}$ 上で2倍した点 $C=(c_x, c_y)$ を暗号文とし、付加情報 $e$ をともに送出する。復号化装置320は、復号化鍵 $p$ 、 $q$ により、暗号文 $C$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{p, q}$ 上で1/2倍し、候補 $M_i$  ( $i=1 \sim 4$ )を求める。その際、4次方程式の解の公式を用いる。候補 $M_i$ より付加情報 $e$ を用いて平文 $M$ を選ぶ。



## 【特許請求の範囲】

【請求項1】 楕円曲線上の演算を利用した一意復号可能な公開鍵暗号方法であって、

2つの素数 $p$ 、 $q$ を生成し、 $n = pq$ を計算し、 $n$ を公開鍵の暗号化鍵、 $p$ と $q$ を秘密鍵の復号化鍵とし、暗号化鍵 $n$ と平文 $M = (m_x, m_y)$ から、平文 $M = (m_x, m_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{n}$ 上で2倍した点 $C = (c_x, c_y)$ を計算して、前記 $C = (c_x, c_y)$ を暗号文とし、かつ、一意復号のための付加情報 $e$ を求め、

復号化鍵 $p$ 、 $q$ と暗号文 $C$ から、4次方程式の解の公式を用いて、暗号文 $C = (c_x, c_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{p, q}$ 上で1/2倍して、平文の候補 $M_i$  ( $i = 1 \sim 4$ )を求め、付加情報 $e$ により、候補 $M_i$  ( $i = 1 \sim 4$ )の中から平文 $M$ を決定することを特徴とする公開鍵暗号方法。

【請求項2】 鍵生成装置、暗号化装置、復号化装置、公開ファイル装置、及び、これら装置を結ぶ通信路から構成され、楕円曲線上の演算を利用した一意復号可能な公開鍵暗号通信システムであって、

前記鍵生成装置は、2つの素数 $p$ 、 $q$ を生成し、該 $p$ 、 $q$ を秘密鍵の復号化鍵として前記復号化装置に記憶する手段と、前記生成した素数 $p$ 、 $q$ の積 $n$  ( $n = pq$ )を計算し、該 $n$ を公開鍵の暗号化鍵として前記公開ファイル装置へ登録する手段とを有し、

前記暗号化装置は、前記公開ファイル装置から暗号化鍵 $n$ を入手し、平文 $M = (m_x, m_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{n}$ 上で2倍した点 $C = (c_x, c_y)$ を計算し、暗号文 $C$ として前記復号化装置に送信する手段と、前記暗号化鍵 $n$ と平文 $M = (m_x, m_y)$ から、ヤコビ記号 $(m_y/n)$ の値 $e_1$ と、 $m_x$ と $1/m_x \pmod{n}$ の大小関係を表わす値 $e_2$ とを求め、一意復号のための付加情報 $e = (e_1, e_2)$ として前記復号化装置に送信する手段とを有し、

前記復号化装置は、前記復号化鍵 $p$ 、 $q$ と暗号文 $C$ から、4次方程式の解の公式を用いて、暗号文 $C = (c_x, c_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{p, q}$ 上で1/2倍して、平文の候補 $M_i = (m_{xi}, m_{yi})$  ( $i = 1 \sim 4$ )を求める手段と、前記候補 $M_i$ の中から $(m_{yi}/n)$ が前記付加情報 $e_1$ と同じ $M_j$  ( $j = 1, 2$ )を選び、該 $M_j$ から前記付加情報 $e_2$ により平文 $M$ を決定する手段とを有する、ことを特徴とする公開鍵暗号通信システム。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】本発明は、デジタル化された情報を伝送する際の暗号方法及び暗号通信システムに関し、詳しくは、楕円曲線上の演算を利用した一意復号可能な公開鍵暗号方法及び公開鍵暗号通信システムに関する。

## 【0002】

【従来の技術】従来の楕円曲線上の演算を暗号化復号化に利用した公開鍵暗号方式としては、楕円曲線 $y^2 \equiv x^3 + b \pmod{n}$ を利用した楕円ラビン方式が知られている例えば、K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, ; "New public-key schemes based on elliptic curves over the ring  $Z_n$ ", Advances in Cryptology-Crypto' 91, LNCS 576, pp. 252-266, 1991参照)。

10 【0003】この楕円ラビン方式は、解読の難しさが素因数分解の難しさと等価であることが数学的に証明されている。しかし、楕円ラビン方式は、暗号化関数が多対一関数なので、暗号文を復号化すると、複数の平文の候補が得られ、受信者にはどれが送信者の送りたい平文なのかわからなかった(復号の多義性)。また、楕円ラビン方式では、復号化にも楕円曲線上の演算を利用しているため、復号化速度が遅かった。

## 【0004】

20 【発明が解決しようとする課題】従来の楕円ラビン方式は、上述の復号の多義性の問題であるので、何らかの付加情報により平文を決定する必要がある。しかしながら、安全性をそなわずに平文を一意に決定するためには、どのような付加情報を送ればよいのかが不明であった。また、復号化速度が遅いことは実用化の際問題となる。

30 【0005】本発明の目的は、従来の楕円ラビン方式と同様に解読の難しさが素因数分解の難しさと等価であり、かつ、簡単に計算できる付加情報により一意に復号が可能であり、かつ、復号化速度がより高速であるような楕円曲線上の演算を利用した公開鍵暗号方法及び公開鍵暗号通信システムを提供することにある。

## 【0006】

【課題を解決するための手段】本発明の楕円曲線上の演算を利用した公開鍵暗号方法及び通信システムは、以下のことを特徴としている。

- (1) 鍵生成では、2つの素数 $p$ 、 $q$ を生成し、 $n = pq$ を計算し、 $n$ を暗号化鍵として公開し(公開鍵)、 $p$ と $q$ を復号化鍵として受信側が秘密に保持する(秘密鍵)。
- 40 (2) 送信側は、平文を $M = (m_x, m_y)$ とし、公開された受信者の暗号化鍵 $n$ と平文 $M$ から、平文 $M = (m_x, m_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{n}$ 上で2倍した $C = (c_x, c_y)$ を計算し、これを暗号文 $C$ として受信側に送信する。また、一意に復号するための情報として、簡単に計算できるヤコビ記号 $(m_y/n)$ の値 $e_1$ と、 $m_x$ と $1/m_x \pmod{n}$ の大小関係を表わす値 $e_2$ とを、暗号文の付加情報として受信側に送信する。
- (3) 受信側は、秘密の復号化鍵 $p$ 、 $q$ により、暗号文 $C = (c_x, c_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{p, q}$ 上で1/2倍する。この1/2倍を計算する際、復



号化をより高速に行うために4次方程式の解の公式を用いる。暗号文Cを1/2倍した点は4つ存在するので、それらを平文の候補 $M_i$  ( $i=1\sim 4$ ) とおく。この $M_i$  ( $i=1\sim 4$ ) の中から、付加情報 $e_1, e_2$ を用いて平文Mを選ぶ。

【0007】

【発明の実施の形態】以下、本発明の一実施の形態について図面を用いて説明する。図1は、本発明の公開鍵暗号方式が適用される通信システムの全体ブロック図を示す。図1において、10はセンタ装置、20は送信側装置、30は受信側装置である。センタ装置10は、利用者から任意に参照可能な公開ファイル装置110を有している。送信側装置20は暗号化装置210を有し、受信側装置30は鍵生成装置310と復号化装置320を有する。

【0008】あらかじめ鍵生成装置310にて、暗号化鍵 $n$ と復号化鍵 $p, q$ を生成し、暗号化鍵 $n$ は公開鍵として公開ファイル装置110に登録し、復号化鍵 $p, q$ は秘密鍵として復号化装置320に記憶しておく。センタ装置10の公開ファイル装置110には、該鍵生成装置310によって生成された暗号化鍵 $n$ が、それぞれ利用者毎に登録されている。

【0009】送信側装置20では、公開ファイル装置110より相手受信者の暗号化鍵 $n$ を入手し、暗号化装置210にて、入力された平文Mを該暗号化鍵 $n$ により暗号化し、さらに付加情報 $e (= e_1, e_2)$ を生成し、その暗号文Cと付加情報 $e$ を受信側装置30に送信する。受信側装置30の復号化装置320では、暗号文Cを復\*

$$\begin{aligned} c_x &= \frac{(3m_x^2 + 1)^2}{(2bm_y)^2} \cdot b - 2m_x \bmod n, \\ &= \frac{(m_x^2 - 1)^2}{4m_x(m_x^2 + 1)} \bmod n, \\ c_y &= \frac{3m_x^2 + 1}{2bm_y} \cdot (m_x - x_3) - m_y \bmod n, \\ &= \frac{(m_x^2 - 1)((m_x^2 - 1)^2 + 8m_x^2)m_y}{2(2m_x(m_x^2 + 1))^2} \bmod n, \end{aligned} \quad (1)$$

【0016】の計算が行われる。ここで、 $b$ の計算は不要であるが、形式的には、 $b = (m_x^3 + m_x) / m_y^2 \bmod n$ を意味する。

【0017】付加情報生成器212は、暗号化鍵 $n$ と平\*

$$e_1 = \left( \frac{m_y}{n} \right), \quad e_2 = \begin{cases} 0, & m_x > (1/m_x \bmod n) \text{ のとき,} \\ 1, & \text{上記以外 のとき,} \end{cases} \quad (2)$$

【0019】の計算が行なわれている。但し、( ) はヤコビ (Jacobi) 記号である。

【0020】暗号化装置210は、求った暗号文C =  $(c_x, c_y)$  と付加情報 $e = (e_1, e_2)$ を受信側装置

\* 号化鍵 $p, q$ と付加情報 $e$ とによって一意に復号し、平文Mを出力する。

【0010】なお、鍵生成装置310は、必ずしも受信側装置30に設ける必要はなく、例えばセンタ装置10に設けてもよいが、この場合には、復号化装置320が保持する復号化鍵 $p, q$ の秘密性が保証される必要がある。

【0011】以下に、鍵生成装置310、暗号化装置210及び復号化装置320の構成例を詳述する。

10 【0012】〈鍵生成装置〉図2は、本発明の一実施例の鍵生成装置310の構成図を示す。素数生成器311は2つの素数 $p, q$ を生成し、乗算器312は $n = pq$ を計算する。ここで、 $n$ は暗号化鍵 (公開鍵) として公開ファイル装置110に登録され、 $p$ と $q$ は復号化鍵 (秘密鍵) として復号化装置320に記憶される。

20 【0013】〈暗号化装置〉図3は、本発明の一実施例の暗号化装置210の構成図を示す。暗号化装置210には、入力として、暗号化鍵 $n$ と平文 $M = (m_x, m_y)$ が与えられる。但し、 $0 < m_x < n$ かつ $0 < m_y < n$ かつ $\gcd(m_x, m_y, n) = 1$ とする。

【0014】楕円曲線2倍算器211は、暗号化鍵 $n$ と平文 $M = (m_x, m_y)$ から、該平文 $M = (m_x, m_y)$ を楕円曲線 $by^2 \equiv x^3 + x \pmod{n}$ 上で2倍した点 $C = (c_x, c_y)$ を計算し、暗号文Cとする。具体的には、楕円曲線2倍算器211では、

【0015】

【数1】

40 ※ 文 $M = (m_x, m_y)$ から、付加情報 $e = (e_1, e_2)$ を計算する。具体的には、付加情報生成器212では、

【0018】

【数2】

30に送出して、動作を終了する。

【0021】〈復号化装置〉図4は、本発明の一実施例の復号化装置の構成図を示す。鍵生成装置310で生成された素数 $p, q$ は各々記憶部321と記憶部322に

記憶されている。

【0022】楕円曲線1/2倍算器323は、楕円曲線  $by^2 \equiv x^3 + x \pmod{p}$  上の暗号文  $C = (c_x, c_y)$  の2つの1/2倍点  $M_{p1} = (m_{xp1}, m_{yp1})$ 、 $M_{p2} = (m_{xp2}, m_{yp2})$  を計算する（復号化）。この場合、よ\*

$$x^4 - 4c_x x^3 - 2x^2 - 4c_y x + 1 \equiv 0 \pmod{p} \quad (3)$$

ここで、 $c_x$  は既知数である。式(3)に4次方程式の解の公式を適用すると、解  $x_i$  ( $i = 1 \sim 4$ ) は形式的に以下ようになる。

$$\begin{aligned} x_1 &= c_{xp} - \sqrt{c_{xp}^2 + 1} - \sqrt{2c_{xp}^2 - 2c_{xp}\sqrt{c_{xp}^2 + 1}} \pmod{p} \\ x_2 &= c_{xp} - \sqrt{c_{xp}^2 + 1} + \sqrt{2c_{xp}^2 - 2c_{xp}\sqrt{c_{xp}^2 + 1}} \pmod{p} \\ x_3 &= c_{xp} + \sqrt{c_{xp}^2 + 1} - \sqrt{2c_{xp}^2 + 2c_{xp}\sqrt{c_{xp}^2 + 1}} \pmod{p} \\ x_4 &= c_{xp} + \sqrt{c_{xp}^2 + 1} + \sqrt{2c_{xp}^2 + 2c_{xp}\sqrt{c_{xp}^2 + 1}} \pmod{p} \end{aligned} \quad (4)$$

【0025】式(4)は少なくとも解  $m_{x_0}$  と  $1/m_{x_0} \pmod{p}$  をもつので、 $x_i$  ( $i = 1 \sim 4$ ) のうち2つは  $m_{x_0}$  と  $1/m_{x_0} \pmod{p}$  である。 $m_{x_0}$  と  $1/m_{x_0} \pmod{p}$  以外の解は  $\pmod{p}$  では存在しないことを示す。

\*り少ない演算量で復号化するために、式(1)を  $\pmod{p}$  に還元した4次方程式を直接解いて1/2点(半点)を計算する。式(1)を  $\pmod{p}$  に還元した式から、解くべき4次方程式は以下になる。

【0023】

※【0024】

【数3】

※

★【0026】具体的に、楕円曲線1/2倍計算器323では、次の計算が行われる。

【0027】

★【数4】

$$\begin{aligned} c_{xp} &= c_x \pmod{p}, \\ c_{yp} &= c_y \pmod{p}, \\ m_{xp1} &= c_{xp} + k_p + \sqrt{2c_{xp}^2 + 2c_{xp}k_p} \pmod{p}, \\ m_{xp2} &= c_{xp} + k_p - \sqrt{2c_{xp}^2 + 2c_{xp}k_p} \pmod{p}, \\ m_{yp1} &= \frac{2(2m_{xp1}(m_{xp1}^2 + 1))^2 c_{yp}}{(m_{xp1}^2 - 1)((m_{xp1}^2 - 1)^2 + 8m_{xp1}^2)} \pmod{p}, \\ m_{yp2} &= \frac{2(2m_{xp2}(m_{xp2}^2 + 1))^2 c_{yp}}{(m_{xp2}^2 - 1)((m_{xp2}^2 - 1)^2 + 8m_{xp2}^2)} \pmod{p}, \end{aligned} \quad (5)$$

【0028】ここで、 $k_p$  は式(6)をみたす値である。

30☆【0029】

☆【数5】

$$k_p^2 \equiv c_{xp}^2 + 1 \pmod{p} \text{ and } \left( \frac{2c_{xp}^2 + 2c_{xp}k_p}{p} \right) = 1 \quad (6)$$

【0030】同様に楕円曲線1/2倍算器324は、楕円曲線  $by^2 \equiv x^3 + x \pmod{q}$  上の暗号文  $C = (c_x, c_y)$  の2つの1/2倍点  $M_{q1} = (m_{xq1}, m_{yq1})$ 、 $M_{q2} = (m_{xq2}, m_{yq2})$  を計算する。

◆  $M_{p1}$ 、 $M_{p2}$ 、 $M_{q1}$ 、 $M_{q2}$  から平文の4つの候補  $M_i = (m_{xi}, m_{yi})$  ( $i = 1 \sim 4$ ) を計算する。具体的には、中国人剰余定理計算器325では、

【0032】

【0031】中国人剰余定理計算器324は、 $p$ 、 $q$  と

◆【数6】

$$\begin{aligned} M_1 &= (m_{x1}, m_{y1}) = (\text{CRT}(m_{xp1}, m_{xq1}), \text{CRT}(m_{yp1}, m_{yq1})), \\ M_2 &= (m_{x2}, m_{y2}) = (\text{CRT}(m_{xp1}, m_{xq2}), \text{CRT}(m_{yp1}, m_{yq2})), \\ M_3 &= (m_{x3}, m_{y3}) = (\text{CRT}(m_{xp2}, m_{xq1}), \text{CRT}(m_{yp2}, m_{yq1})), \\ &= (1/m_{x2} \pmod{n}, -m_{y2}/m_{x2}^2 \pmod{n}), \\ M_4 &= (m_{x4}, m_{y4}) = (\text{CRT}(m_{xp2}, m_{xq2}), \text{CRT}(m_{yp2}, m_{yq2})), \\ &= (1/m_{x1} \pmod{n}, -m_{y1}/m_{x1}^2 \pmod{n}). \end{aligned} \quad (7)$$

【0033】の計算が行なわれる。ここで、 $\text{CRT}(t_0, t_1)$  は  $t_0$ 、 $t_1$  に中国人剰余定理を適用することを

意味し、具体的には、式(8)で表わされる。

\*【数7】

【0034】

\*

$$\text{CRT}(t_p, t_q) = t_p \cdot (1/q \bmod p) \cdot q + t_q \cdot (1/p \bmod q) \cdot p \bmod pq \quad (8)$$

【0035】比較器326では、 $e_1$ を用いて、 $M_i = (m_{x,i}, m_{y,i})$  ( $i = 1 \sim 4$ )の中から $(m_{y,i} / pq)$ が $e_1$ と同じ点を選ぶ。このような $M_i$ は必ず2つある。それらを $M_1, M_2$ とおく。次に、比較器327において、 $e_2$ を用いて、 $M_1$ と $M_2$ のうち、 $e_2 = 0$ ならばx座標値が大きい方、さもなければx座標値が小さい方を平文Mとして出力する。

【0036】

【発明の効果】上述のように、本発明の公開鍵暗号方法及び公開鍵暗号通信システムによれば、解読の難しさが素因数分解の難しさと等価であり、即ち、全面的に解読することは暗号化鍵nを素因数分解することと等価であり、かつ、簡単に計算できる付加情報により一意に復号が可能であり、さらに、復号に4次方程式の解の公式を利用することにより、復号化速度のより高速化が可能である。

【図面の簡単な説明】

【図1】本発明の一実施例のシステム全体図である。

【図2】鍵生成装置の一実施例の構成図である。

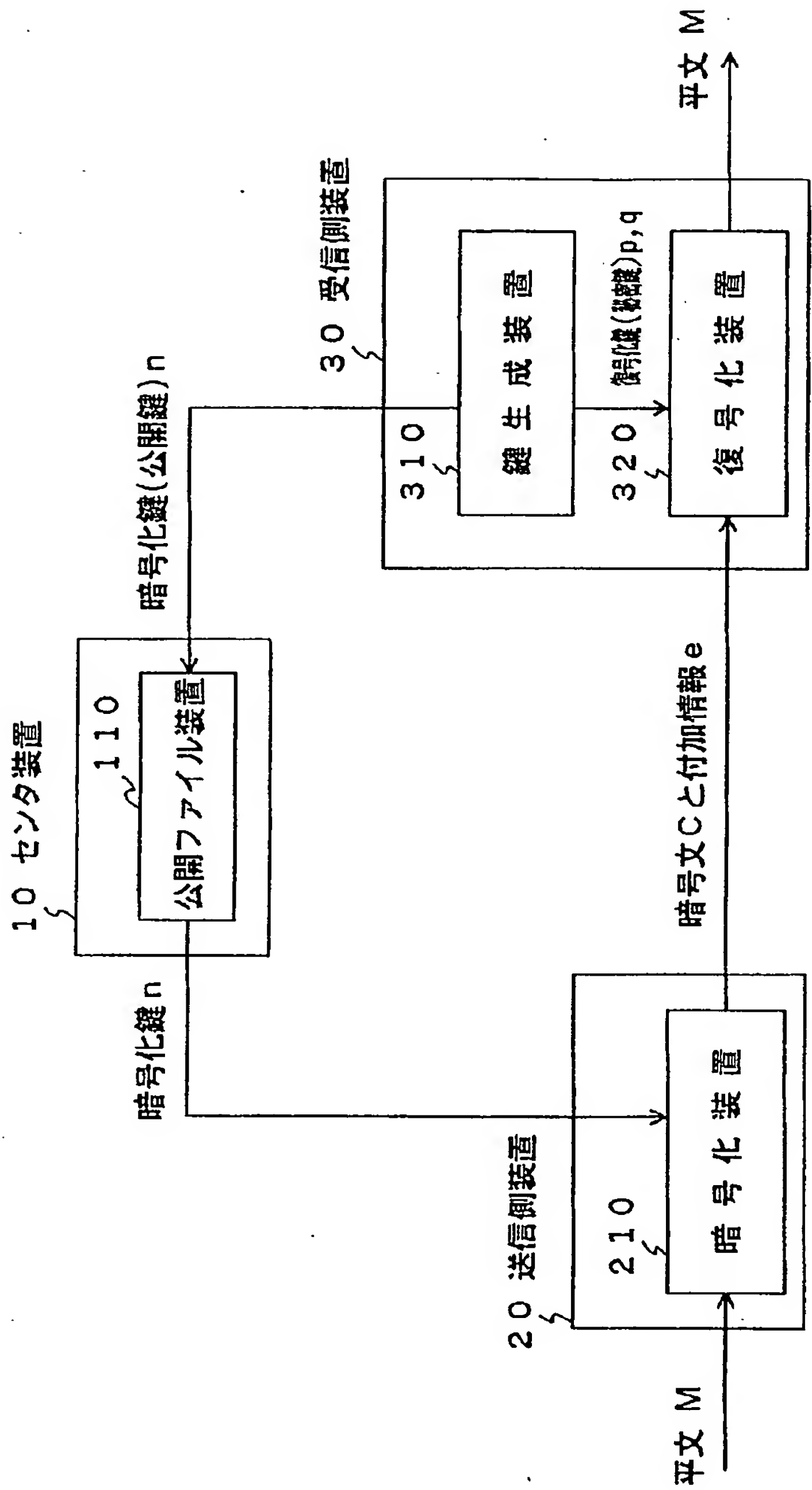
【図3】暗号化装置の一実施例の構成図である。

【図4】復号化装置の一実施例を構成図である。

【符号の説明】

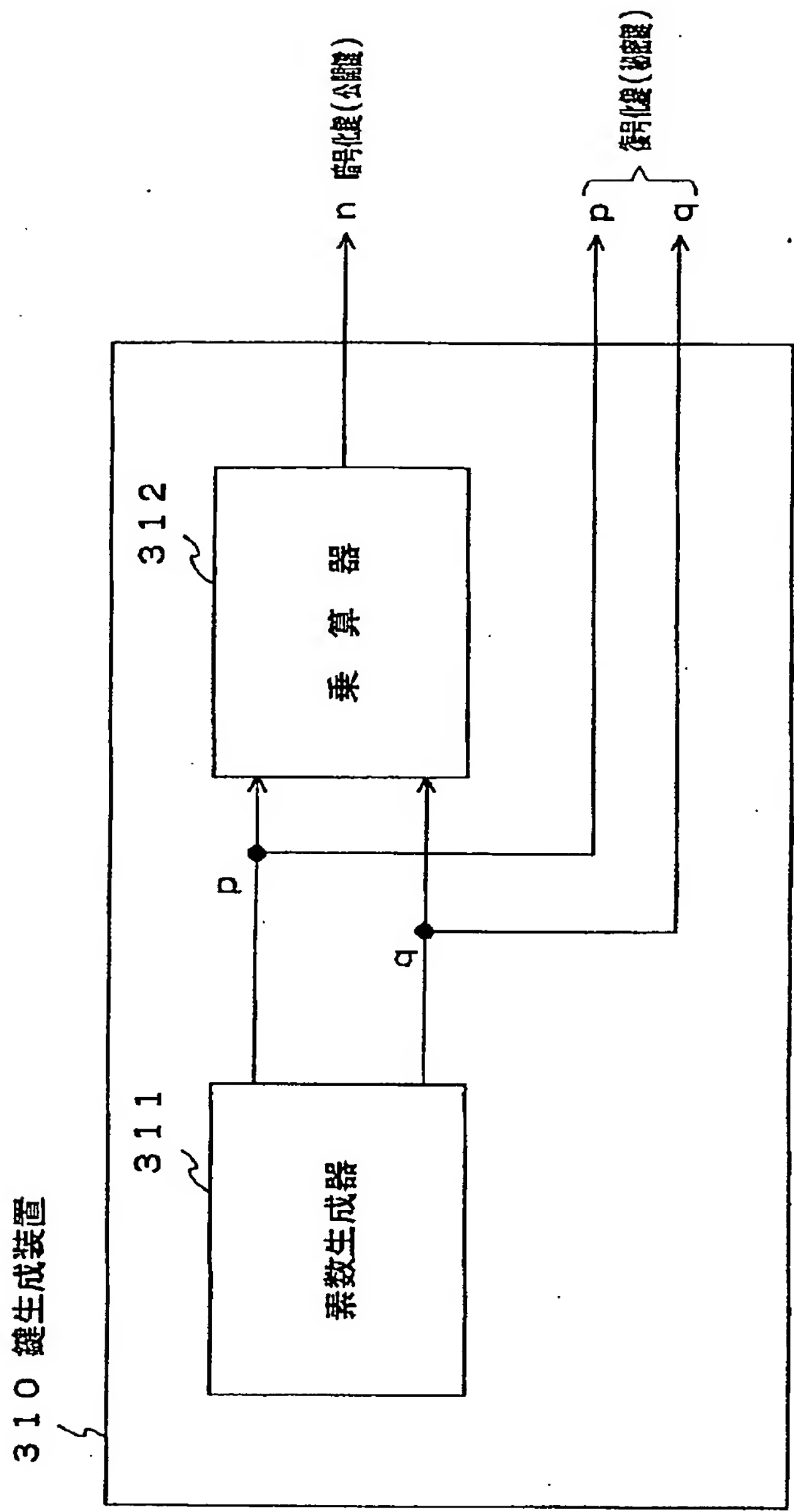
- |          |            |
|----------|------------|
| 110      | 公開ファイル装置   |
| 210      | 暗号化装置      |
| 211      | 楕円曲線2倍算器   |
| 212      | 付加情報生成器    |
| 310      | 鍵生成装置      |
| 311      | 素数生成器      |
| 312      | 乗算器        |
| 320      | 復号化装置      |
| 321, 322 | 秘密鍵記憶部     |
| 323, 324 | 楕円曲線1/2倍算器 |
| 325      | 中国人剰余定理計算器 |
| 326, 327 | 比較器        |

【図1】

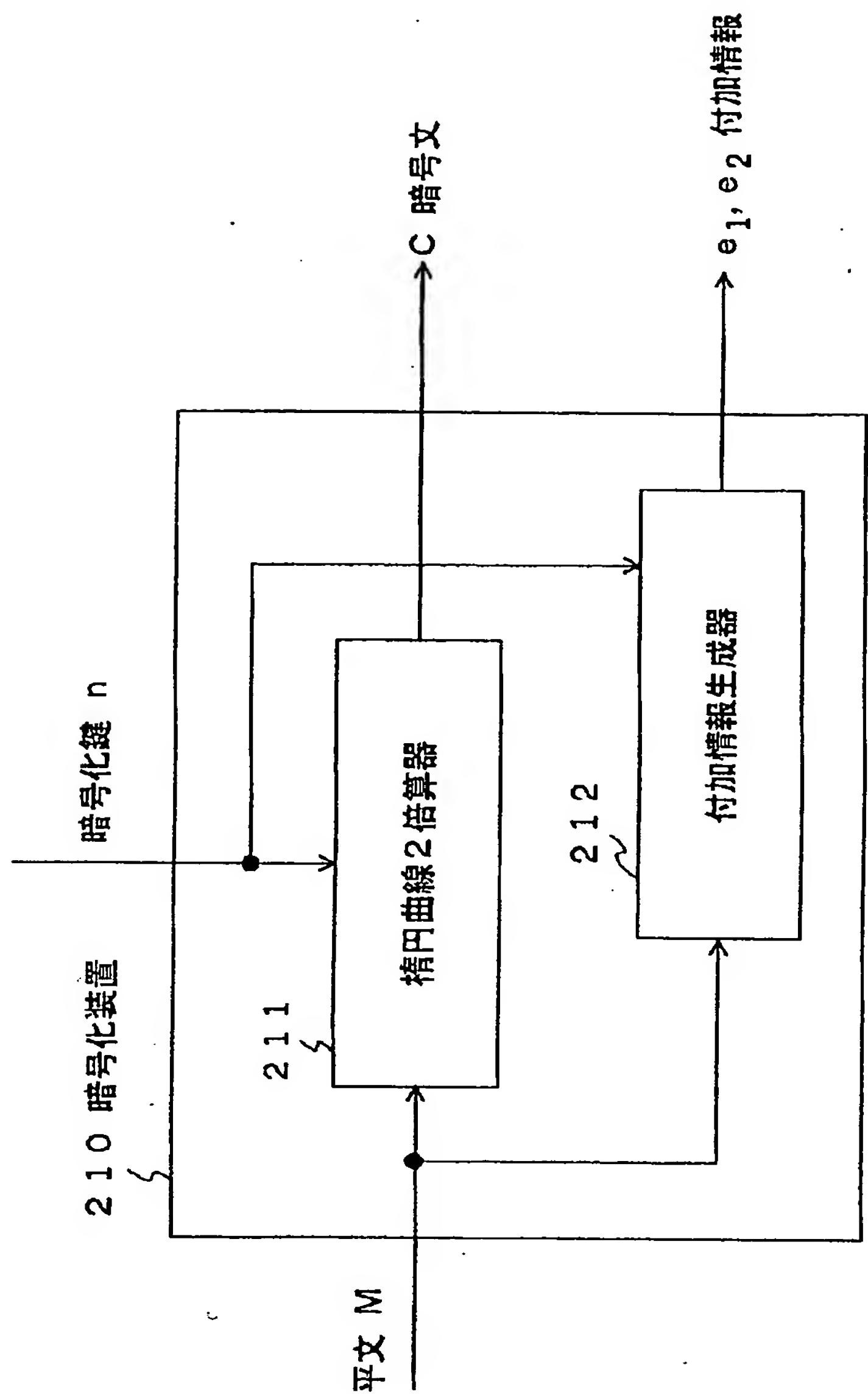




【図2】



【図3】



【図4】

